Kevad 2015

Märkusi arvuteooria 10. praktikumi kohta:

A. Kommentaare ülesannete kaupa:

1. Lihtsaim ent töömahukaim võimalus oli lihtsalt järgemööda 7, 11, 15 ja 21 astmed välja arvutada, kuni tulemuseks tuleb 1 modulo 22. Vastav astendaja ongi jäägiklassi järk. Seda tegevust saab optimeerida Lagrange'i teoreemi abil, mille kohaselt järgud võivad olla vaid

$$\varphi(22) = 10$$

jagajad, st. kas 1, 2, 5 või 10. Seega on vaja leida vaid 2. ja 5. aste, sest 10. aste on Euleri teoreemi kohaselt alati kongruentne ühega. Algjuur on antud juhul siis 10. järku element, ja selleks sobib vaid 7. Jäägiklassi $\overline{15}$ järk on 5, $\overline{11}$ ei ole üldse pööratav, seega tal järku ei ole, ja $\overline{21} = -\overline{1}$ järk on 2. Viimane asjaolu kehtib muuseas alati, sest ilmselt $(-\overline{1})^2 \equiv 1$ ja $-\overline{1} \not\equiv 1$. See ongi see üksainus 2. järku element, millele viitab loengukonspekti lemma 7.5.

2. Siin oli vaja tähele panna, et ülesanne taandus kongruentside

$$2^x \cdot a \equiv a \pmod{41}$$

samaaegsele lahendamisele kõigi $a \not\equiv 0 \pmod{41}$ jaoks. Kuna 41 on algarv, siis $\overline{a}$ on pööratav ja tegelikult on vaja lahendada vaid kongruents $2^x \equiv 1 \pmod{41}$ ehk leida elemendi $\overline{2}$ järk rühmas $\mathbb{Z}_{41}^*$. See on 20 (ja 2 ei ole järelikult algjuur), mistõttu kaarte tuleb segada mistahes 20 kordne arv (20, 40, 60 jne) kordi.

3. Jälle sai kasutada Lagrange'i teoreemi ja leida vaid need astmed, mis on $\varphi(16) = 8$ jagajateks. Muuseas iga mittepööratava elemendi astmed on alates mingist kohast kongruentsed nulliga, näiteks $10, 10^2 \equiv 4, 10^3 \equiv 8, 10^4 \equiv 0, 10^5 \equiv 0$ jne.

4. Töömahukam variant on leida kõigi pööratavate elementide järgud samal viisil, kui ülesandes 1. Siis $\varphi(n)$ järku elemendid ongi otsitavateks algjuurteks. Kavalam oli kasutada järgmise loengu materjali ja panna tähele, et ühte konkreetset algjuurt on võimalik efektiivsemalt leida järelduse 7.21 abil, kusjuures algjuuri on teoreemi 7.24 tõttu kokku $\varphi(\varphi(n))$ tükki (kui neid muidugi

üldse leidub). Näiteks juhul $n = 10$ on $\varphi(10) = 4$ (ehk meil on 4 pööratavat elementi) ja $\varphi(4) = 2$ (ehk kaks neist on algjuured). Kuna ilmselt $\overline{1}$ ja $-\overline{1}$ ei saa olla algjuurteks, sest nad on vastavalt 1. ja 2. järku, siis peavad algjuured olema ülejäänud pööratavad elemendid, st. 3 ja 7.

Alternatiivina võis rakendada järeldust 7.10, mille abil saab kõik algjuured avaldada ühe algjuure astmetena. Näiteks juhul $n = 11$ on eelneva metoodikaga kontrollitav, et 2 on algjuur. Seetõttu on ülejäänud algjuurteks 2 sellised astmed, mille suurim ühistegur arvuga $11 - 1 = 10$ on 1, ehk $2^3 \equiv 8, 2^7 \equiv 7$ ja $2^9 \equiv 6 \pmod{11}$.

Ülejäänud vastused: mooduli 9 järgi on algjuurteks 2 ja 5, mooduli 12 järgi algjuuri ei ole ja mooduli 14 järgi on algjuured 3 ja 5.

5. Lihtne ülesanne, mida võis lahenda vastuväiteliselt või lemma 7.3 abil. Ainus raskus seisnes siin selle meeles pidamisel, et $a^k \equiv 1 \pmod{n}$ parajasti siis, kui $\overline{a}$ järk on maksimaalselt k, MITTE võrdne k-ga.

6. Sisuliselt taandus ülesanne tõestamisele, et $\overline{2}$ järk mooduli $2^n - 1$ järgi on n. Veidi raskusi valmistas näitamine, et kui $1 \leq m < n$, siis

$$2^m \not\equiv 1 \pmod{2^n - 1}.$$

Selleks piisas, kui panna tähele, et $1 < 2^m \leq 2^n - 1$ ja kasutada lauset 3.6.

7. Siin tuli avaldada arvud $1, \ldots, p-1$ mingi algjuure a astmetena ja leida saadud geomeetrilise rea summa (seejuures kasutades asjaolu, et $a^n \not\equiv 1 \pmod{p}$ tänu lemmale 7.3).

8. Jälle sai teha eelmises ülesandes esinenud asenduse mingi algjuure a astmetega. Seega on otsitav summa kongruentne arvuga

$$S = a^{\frac{p(p-1)}{2}}$$

mooduli p järgi. Arvu S ruut on selgelt kongruentne ühega, seega lause 2.9 kohaselt (võrrand $x^2 - 1$ omab vaid lahendeid $\overline{1}$ ja $-\overline{1}$) peab kehtima $S \equiv \pm 1 \pmod{p}$. Juht $S \equiv 1 \pmod{p}$ ei sobi, sest järelduse 5.14 tõttu

$$a^{\frac{p(p-1)}{2}} \equiv (a^{\frac{p-1}{2}})^p \equiv a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}.$$

Tõepoolest, vastasel juhul oleks a järk ülimalt $\frac{p-1}{2}$, aga a on algjuur ja tema järk on $p - 1$. Järelikult $S \equiv -1 \pmod{p}$, nagu soovitud.